

What is claimed is:

1. A data storage comprising:
a first storage area for storing an original version of management information; and
5 a second storage area for storing an encrypted version of the management information.
2. A method for manufacturing a data storage comprising the steps of:
writing an original version of management information into a first storage area in
10 the data storage; and
writing an encrypted version of the management information into a second storage area in the data storage.
3. A process carried out in an information processing system comprising:
15 reading an original version of management information stored on the data storage to be verified and an encrypted version of the management information;
decrypting the encrypted version of the management information; and
comparing the original version of the management information and the decrypted management information,
20 wherein the data storage subjected to verification is determined as valid when the comparison result indicates that the original version of the management information and the decrypted management information are in a predetermined relationship with each other.
4. A method as claimed in Claim 3, wherein the encrypted version of the management
25 information is encrypted with an encryption scheme using secret key information and the decryption is performed with that secret key information.
5. A system for verifying the validity of a data storage having a first storage area for storing an original version of management information and a second storage area for storing

an encrypted version of the management information, said system comprising:

a controlling unit adapted to read the original version of the management information and the encrypted version of the management information out of the data storage and control decryption of the encrypted version of the management information; and

5 a comparing unit adapted to determine whether the original version of the management information and the decrypted management information are in a predetermined relationship with each other and validate the data storage when the determination result is affirmative.

10 6. A method for managing a user terminal performed in a content distribution server adapted to deliver content data to a user terminal in response to a request from the user terminal connected to the content distribution server through a network, said method comprising:

requesting the user terminal to send an original version of management information
15 and an encrypted version of the management information, the original and encrypted versions of the management information being stored on the data storage in the user terminal;

receiving the original and encrypted versions of the management information;

decrypting the received encrypted version of the management information;

20 determining whether the received original version of the management information is in a predetermined relationship with the decrypted management information; and

validating the management information when the determination result is affirmative, wherein

a predetermined request from the user terminal is fulfilled when the determination
25 result is affirmative.

7. A method as claimed in Claim 6, further comprising:

determining whether the management information of which validity has been verified is contained in a predetermined management information list, wherein

fulfillment of a predetermined request from the user terminal is limited when the determination result is affirmative.

8. A method as claimed in Claim 7, wherein the predetermined management information list is a collection of management information for the user terminal(s) to which a content data file is to be delivered.

9. A content distribution server adapted to deliver content data to a user terminal in response to a request from the user terminal connected to the content distribution server through a network, said content distribution server comprising:

an interface for the transmission of data to and from the content distribution server through the network;

a controlling unit that makes a request to send an original version of management information and an encrypted version of the management information through said interface, the original and encrypted versions of the management information being stored on the data storage in the user terminal, and that controls decryption of the received encrypted version of the management information; and

a comparing unit adapted to determine whether the original version of the management information and the decrypted management information are in a predetermined relationship with each other and validate the management information when the determination result is affirmative, wherein

said controlling unit limits the delivery of the content data to the user terminal when the verification result is negative.

10. A content distribution server adapted to deliver content data to a user terminal in response to a request from the user terminal connected to the content distribution server through a network, said content distribution server comprising:

an interface for the transmission of data to and from the content distribution server through the network;

a controlling unit that makes a request to send an original version of management information and an encrypted version of the management information through said interface, the original and encrypted versions of the management information being stored on the data storage in the user terminal, and that controls decryption of the received encrypted version
5 of the management information;

a first comparing unit adapted to determine whether the original version of the management information and the decrypted management information are in a predetermined relationship with each other and validate the management information when the determination result is affirmative;

10 a management information database which is a collection of pieces of management information for the data storage to which delivery of the content data is limited; and

a second comparing unit adapted to determine whether the management information of which validity has been verified is contained in a predetermined management information database, wherein

15 said controlling unit permits the delivery of the content data when the verification result obtained by said first comparing unit is affirmative and when the determination result obtained by said second comparing unit is negative.

11. A computer program for use in making an information processing system carry out
20 the jobs of:

writing an original version of management information into a first storage area in a data storage; and

writing an encrypted version of the management information into a second storage area in the said data storage.

25 12. A computer program for use in making an information processing system carry out the jobs of:

reading an original version of management information and an encrypted version of the management information out of the data storage to be verified;

decrypting the encrypted version of the management information;

comparing the read original version of the management information and the
decrypted management information; and

validating the verified data storage when the comparison result indicates that the
5 read original version of the management information and the decrypted management
information are in a predetermined relationship with each other.

13. A computer program for use in making a content distribution server, which is
adapted to deliver content data to a user terminal in response to a request from the user
10 terminal connected to the content distribution server through a network, carry out the jobs
of:

requesting delivery of an original version of management information and an
encrypted version of the management information stored in a data storage of the user
terminal;

15 receiving the original and encrypted versions of the management information;
decrypting the received encrypted version of the management information;
determining whether the received original version of the management information
and the decrypted management information are in a predetermined relationship with each
other; and

20 either validating the management information when the determination result is
affirmative or limiting fulfillment of any request from the user terminal when the
verification result is negative.

14. A computer-readable data storage having the computer program as claimed in
25 Claim 11 stored thereon.

15. A computer-readable data storage having the computer program as claimed in
Claim 12 stored thereon.

16. A computer-readable data storage having the computer program as claimed in Claim 13 stored thereon.

205210" 254/500T